The Role of Personalized Services and Control: An Empirical Evaluation of Privacy Calculus and Technology Acceptance Model in Mobile Context

Zhan Liu[a], Jialu Shan[b], Yves Pigneur[c]

[a]Institute of Information Systems, University of Applied Sciences and Arts Western Switzerland (HES-SO Valais-Wallis), Sierre, Switzerland, zhan.liu@hevs.ch; [b]Global Center for Digital Business Transformation, International Institute for Management Development (IMD Business School); [c]Faculty of Business and Economics (HEC), University of Lausanne

This is a preprint of an article whose final and definitive form has been published in the Journal of Information Privacy and Security, 2016, VOL 12, NO. 3, 123-144. http://dx.doi.org/10.1080/15536548.2016.1206757 Journal of Information Privacy and Security is available online at: http://www.tandfonline.com/toc/uips20/current

Abstract

The last few years have witnessed an explosive growth in the use of smartphones. Such widespread use brings with it concerns over the protection of privacy. Building upon existing privacy concern literature, this study has developed a theoretical framework that combines a privacy calculus model with a technology acceptance model (TAM) in the mobile application context. Also examined is the role of personalized services and users' perceived information control in this domain. Based on a study of 308 participants, the results reveal that perceived enjoyment has replaced perceived ease-of-use as a main predictor of perceived behavioral intentions in a mobile TAM. The findings also show that personalized services and users' perceived information control have a strong effect on both privacy calculus and mobile TAM.

Keywords: Personalization, Control, Privacy calculus, Mobile TAM, Perceived enjoyment, Privacy

Introduction

The recent explosive growth in information technology and digital networks, particularly the prominent growth in the popularity of smartphones and tablets, has fuelled the debate that surrounds the issue of privacy protection (Dhar and Varshney, 2011; Dinev and Hart, 2004; Keith et al., 2013). Unlike traditional market transactions, exchanges in the mobile context usually do not involve face-to-face interactions. Rather, the behavioral intentions of companies that collect personal data are not always clear to mobile users. A recent study conducted by Sutanto et al. (2013) indicated that smartphones such as iPhones and Android phones can secretly track user information; indeed, half of all iPhone applications are capable of so doing. As a result, concerns over information privacy have become a real issue in m-commerce. In particular, they have attracted the attention of information system researchers.

Information privacy usually refers to the interest that people have in controlling, or at least significantly influencing, the handling of information about themselves (Bélanger and Crossler, 2011; Clarke, 1999). As e-commerce and more recently m-commerce continue to grow worldwide, companies collect increasingly large amounts of personal information from Internet and mobile users. This consumer data is then used to develop more efficient and effective marketing strategies. To build these databases, however, customers are required to share their personal information with companies, whether voluntarily or involuntarily (Graeff and Harmon, 2002; Nam et al., 2006). In fact, consumers can reasonably expect to have to provide companies with a certain level of personal purchase information in order to enjoy individualized and personalized transactions. New advances in tracking technologies in m-commerce enable marketers to construct personal profiles and use them to tailor their advertising messages for mobile users even more precisely than for other online customers (King and Jessen, 2010).

The majority of research has been based on online commercial exchanges. As such, it has not examined whether such operations give rise to the same consumer privacy concerns as transactions that take place in the mobile context. From both theoretical and practical perspectives, it is important to better understand the personalization-privacy paradox in the context of mobile activities, because Internet use in general might not completely reveal the perceptions and attitudes that are associated with the use of different smartphone applications.

Thus, the purpose of this paper is to examine the relationship between beliefs about information privacy and mobile application usage intentions. Specifically, *how do mobile users perceive information privacy when using location-based applications, and how do such perceptions affect their intention to use these applications?* Moreover, in this paper, we will also consider the possible impacts of users' control over the release of private information and the personalized services provided by applications in these relationships.

To answer these questions, we established a theoretical model that is based on both a privacy calculus and technology acceptance model. More importantly, it incorporates personalization and perceived information control as two important factors on both models. On the one hand, therefore, we aim to examine whether the personalized characteristics of mobile applications would meet users' personal needs more effectively, leading to more positive results (i.e., increased perceived benefit). On the other hand, we intend to demonstrate whether perceived information control can promote users' psychological comfort (i.e., reduced perceived risks) and thus increase their willingness to disclose data, and whether such a solution would also impact on their intention to use mobile applications.

The rest of this paper is organized thus: the next section provide a theoretical foundation and offer hypothesis development for this research. A methodology section is then presented, which describes the data collection process and sample taken, and reports on the testing of our hypotheses. Following a discussion of the main findings and implications, we report its contribution and limitations. Finally, this paper concludes with a brief summary.

Theoretical Model and Hypothesis Development

Privacy Concerns and Privacy Calculus

Information privacy concerns refer to an individual's subjective concerns within the context of information privacy (Malhotra et al., 2004). Such concerns have often been cited as one of the key reasons for consumers failing to make purchases over the Internet (George, 2004). More importantly, individuals view privacy problems differently. Ackerman (2004) argued that such differences came from two main sources: types of concerns, and degree of concerns among people. Smith et al. (1996) identified four kinds of information privacy concerns, namely 1) collection; 2) unauthorized

secondary use; 3) improper access and 4) errors. Hong and Thong (2013) raised two dimensions: control and awareness. People are concerned whether they have adequate control over their personal information, and they are also worried about their awareness of information privacy practices. In a more recent study, Liu et al. (2014) confirmed that Smith et al. (1996)'s four types of privacy concerns also prevail in the mobile context. In addition, they raised three additional considerations: agreement on information releasing, reputation consideration and legal consideration. While the first two elements are associated more with the organizational perspective, the last one takes a regulation and governmental policy perspective. Moreover, their results showed the important roles of personalization and control over personal information in smartphone users' privacy calculus of, as well as the user's mobility and the risk attitude have the strong influence on their perceived usefulness.

Consumers, on the other hand, are not one homogenous group; rather, they hold very different opinions on privacy concerns. Some people might be indifferent to privacy, while some are extremely uncompromising. Ackerman et al. (1999) labeled these two groups as marginally concerned and privacy fundamentalist; in between the two, he saw a third group known as the pragmatic majority. Spiekermann et al. (2001) separated the pragmatic majority identified by Ackerman et al. (1999) into two distinct groups according to the focus of their different privacy concerns. Those in the first group have "identity concerns", focusing on the revelation of identity aspects such as name, address or email. The second group is "profiling averse", and are more concerned with the profiling of their interests, hobbies, health and other personal information. In all these studies, different groups showed significantly different degrees of concern over the potential disclosure of personal data in online situations such as e-commerce.

Prior studies on information privacy have repeatedly found that individuals are willing to disclose personal information in exchange for some economic or social benefit (e.g., Dinev and Hart, 2006a; Keith et al., 2013). This leads to a risk-benefit trade-off analysis, or a privacy calculus; in other words, a determination about whether to disclose information after weighing factors related to how that information will be used (Dinev and Hart, 2007). Keith et al. (2013) argued that it is a "rational theory that seeks to explain the attitudes, beliefs, intentions, and behaviors of IT consumers when the use of the IT includes the cost of a perceived privacy risk" (p.1165). They found that only a weak significant relationship existed between mobile device information disclosure intentions and actual information disclosure. Moreover, this relationship was heavily moderated by the consumer practice of disclosing false data. Their results suggested that perceived privacy risks play a larger role than perceived benefits in determining disclosure intentions.

According to privacy calculus, a user's intention to disclose information depends on two key concepts: perceived risks and perceived benefits. The anticipation of benefits is expected to have a positive influence on an individual's intention to disclose personal information. Such benefit may be either monetary or non-monetary. For instance, Hann et al. (2002) provided evidence that individuals

were willing to trade off privacy concerns for economic returns. Phelps et al. (2000) found that direct marketing consumers were willing to exchange personal information for shopping benefits such as future shopping time and effort savings. In the context of e-commerce and m-commerce, empirical results reached a similar conclusion. For example, Nam et al. (2006) found that Internet users tend to feel more secure and safe with websites that they perceive to be more comfortable, convenient and easy to use. In turn, this positively affects a user's intention to disclose information. Xu et al. (2010) identified two anticipated benefits in using a location-based service (LBS), locatability and personalization, both of which could amplify a user's desire to engage in a LBS transaction. They integrated the justice theories into the privacy calculus model and studied the efficacy of the three privacy intervention strategies, compensation, industry self-regulation, and government regulation in influencing individual privacy decision making. They found that perceived privacy risks reduce disclosure intentions, however perceived benefits of information disclosure increase intentions. The individual's privacy calculus very based on the type of information delivery mechanism, such as pull and push.

Expected potential risk, on the other hand, is predicted to be negatively related to the intention to disclose personal information. A number of studies have examined the risk as an antecedent to intentions to conduct transactions (e.g., Dinev and Hart, 2006a, Dinev and Hart., 2006b; Malhotra et al., 2004). In fact, risks are everywhere. They exist just as much in conventional high street commerce. When a consumer buys a product, a certain amount of risk about the quality of that product is involved. Nevertheless, the more information technology has come to be used to facilitate transactions, the greater is the risk associated with the disclosure of personal information (Dinev and Hart, 2006a). In the context of the mobile world, where so-called LBS can pinpoint the whereabouts of mobile users, the threat to individual privacy assumes even greater significance. The uniqueness of LBS and its real-time location data nature has led to predictions that it will become the "killer application" of mobile commerce (Junglas and Watson, 2008). However, the use of LBS to continuously collect and utilize users' real-time location data means that privacy risks will persist, with a wide range of threats, from simple annoyance to outright personal danger (Keith et al., 2013).

Unfortunately, with few exceptions (e.g., Keith et al., 2013; Xu et al., 2010), there is a distinct lack of relevant studies. Thus, it is particularly timely that we seek to gain a better understanding of information disclosure in the context of mobile applications. In the present study, we do not formally hypothesize the privacy calculus-based relationship, as it has been widely tested in previous studies. Our emphasis is on the role of personalization and perceived information control, and on individuals' disclosure intentions, whether or not through a change in perceived risks or perceived benefits.

Technology Acceptance Model and M-Commerce

In the same way that a website offers online purchasing, a smartphone can act as a mobile computer; in essence, it is a form of information technology. As a result, individuals' intentions to use products and service via mobiles can be explained in part, if not fully, by the technology acceptance model (Davis 1989; Davis et al., 1989). This model provides sound predictions of usage by linking behaviors to attitudes and beliefs. It asserts that the intention to use and actual use of an information system are primarily dependent on two particular beliefs: perceived usefulness and perceived ease-of-use (see Figure 1). *Perceived usefulness* is defined as "*the degree to which a person believes that using a particular system would enhance his or her job performance*" (Davis, 1989, p.320) and perceived ease of use refers to "the degree to which a person believes that using a particular system would be free of effort" (Davis, 1989, p.320). In addition, TAM theory proposes that the latter positively influences the front construct.

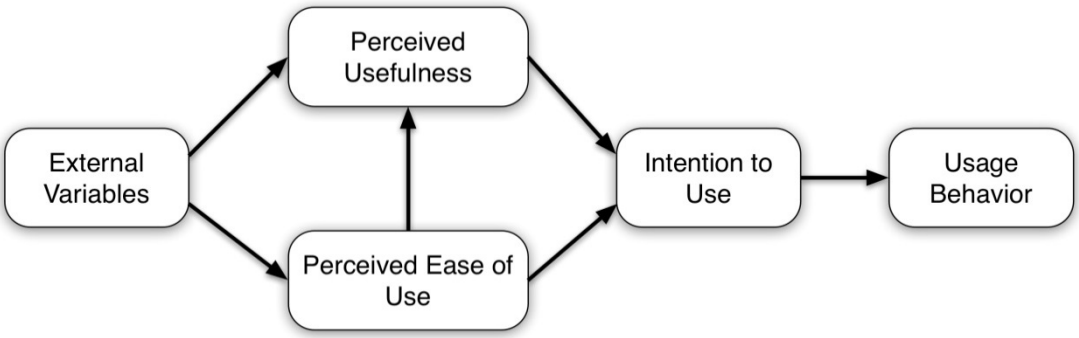

Figure 1. Technology acceptance model (TAM, Davis, 1989; Davis et al., 1989)

Since its inception, the TAM has been widely applied to a diverse set of information technologies and users, and a body of empirical research has supported its propositions (e.g., Adams et al., 1992; Gefen et al., 2003; Van der Heijden, 2004; Venkatesh and Davis, 2000). Across these empirical tests, perceived usefulness has consistently been a strong determinant of usage intentions (the regression coefficients are typically around 0.6), with a weaker effect of another important determinant - perceived ease-of-use. A smartphone, however, is more than just an IT interface. In mobile commerce, typically in a location-based service environment, users are more engaged. They generally get such benefits as LBS resources, discount coupons or monetary awards from a company or service provider by disclosing their location with a certain degree of accuracy (Chorppath and Alpcan, 2013). However, disclosing location information brings huge risks for individuals, as a mobile device is more personal than a desktop computer. Consequently, mobile users have to compromise their privacy in order to bring user experience benefits. Moreover, mobile devices also store additional personal information, such as personal contacts, sent or received messages, emails, photos, and other information. Many mobile applications can automatically access and collect such information, which

personally identifies an individual. Consequently, they can use this information for other purposes. Thus, a smartphone is not usually seen as a trustworthy and reliable source of product and service information.

Furthermore, scholars have extended the original TAM to other areas, such as hedonic information systems (e.g., van der Heijden, 2004), online shopping (e.g., Gefen et al., 2003), a consumer context (e.g., Venkatesh et al., 2012), an e-service context (e.g., Xu et al., 2013), and newly developed mobile applications (e.g., Liu et al., 2014). Among those extended models, perceived enjoyment (sometimes called hedonic motivation) appears to be an important determinant of behavioral intention and perceived ease of use. Unlike perceived usefulness, which focuses on extrinsic motivation, perceived enjoyment focuses on intrinsic motivation (van der Heijden, 2004). It specifies the degree to which fun can be derived through the use of technology or a particular service (Xu et al., 2013). Given the hedonic aspects of mobile-based applications and services, it is appropriate to capture a hedonic perspective in addition to a utilitarian one (perceived usefulness).

Based on the previous findings, we put forward the idea that, in addition to the original two main predictor variables of the TAM (perceived usefulness and perceived ease-of-use), perceived enjoyment has been playing an increasingly important role in voluntary mobile usage situations. Thus, in this study, we have also included the mobile TAM context. We are now in a position to propose the first set of hypotheses as follows:

Hypothesis 1a: The level of perceived usefulness is positively related to mobile user's intention to use.

Hypothesis 1b: The level of perceived ease-of-use is positively related to mobile user's intention to use.

Hypothesis 1c: The level of perceived enjoyment is positively related to mobile user's intention to use.

Hypothesis 1d: The level of perceived ease-of-use is positively related to mobile user's perceived usefulness.

Although the previous literature has shown that perceived usefulness and perceived ease of use as a primarily determinants in the behavioral usage intention, privacy calculus can also influence, especially for LBS mobile applications where user's contextual information is collected. Pomery et al. (2009) argued that behavioral willingness reflects an individual's openness to opportunity, that is his or her willingness to perform a certain behavior in situation that are conducive to that behavior. In fact, some previous studies have documented that user's willingness to disclose personal information could be explained the consumers have an idea of how they might react in risky situations (Anderson and Agarwal, 2011; Dinev and Hart, 2006a). A higher level of willingness to provide personal information, therefore, indicates an intensive motivation to use the services for mobile users. In other

words, users' willingness to provide personal information would influence their intentions to user the application. Moreover, research found that consumers indicated a willingness to provide information in exchange for some benefits and interests such as conveniences and time savings (e.g., Phelps et al., 2000; Dinev and Hart, 2006a). These findings suggested that mobile users willingly to provide their information because they wanted to enjoy the benefit of certain application, indicating their intentions in continuing to use of the application.

By linking a privacy calculus and the mobile TAM, we are able to propose that users' willingness to disclose data has a strong positive effect on users' intentions to use mobile applications. Thus,

Hypothesis 2: The level of a user's willingness to share or disclose data is positively related to mobile user's intention to use.

The Effect of Personalization

Personalization can be defined as "the ability to proactively tailor products and product purchasing experiences to tastes of individual consumer based upon their personal and preference information" (Chellappa and Sin, 2005). Although this definition has its basis in an online setting, a common theme can also be found in the context of the mobile world: personalization is adaptive (Sheng et al., 2008). In particular, it is an interactive process in which a service provider offers relevant customized content based on consumer's individual preferences.

Therefore, personalization is critically dependent on two factors: the ability of firms to acquire and process consumer information, and consumers' willingness to share information and use personalization services (Chellappa and Sin, 2005). From a company's perspective, improvements in personalized services would increase customer satisfaction levels and customers' intentions to repurchase. In turn, this would result in improved company profitability (Kim and Lee, 2009). Today's advancements in networks, applications and devices in the m-commerce environment mean that an enormous amount of information, including real-time data, will become available to service providers. As a consequence, the ability of firms to provide individual care and attention, including personalization, has become a key competitive necessity.

From the customer's point of view, there are two sides to personalization. First, personalization affects information processing and the decision outcomes of customers (Tam and Ho, 2006). With the plethora of choices available in today's business environment, customers are willing to benefit from any tailored information (e.g., advertisement) and services in order to receive potential cost savings (e.g., searching cost). In the m-commerce context, mobile customers disclose their personal information in return for something that has a contextualization value, such as promotional information that is based on their interests, activities, identity, location and the time of the day (Dey and Abowd, 2000; Junglas and Watson, 2006). Second, personalization is gained only in cases when customers have provided their personal information and location data. Existing social behaviors

literature has shown that consumers incur privacy costs when they directly or indirectly provide personal information to a company. There is no precise value to such a social exchange (Awad and Krishnan, 2006); however, there is a kind of trade-off between personalization and loss of privacy. Some researchers call this dilemma a *personalization-privacy paradox* (e.g., Sheng et al., 2008; Sutanto, et al., 2013; Xu et al., 2011).

It has been suggested by prior studies that personalization has been found to be positively associated with perceived benefit (e.g., Chellappa and Sin, 2005; Xu et al., 2011; Liu et al., 2011). Consequently, it can lead to a higher level of intention to use personalized services, and can influence actual future behaviors. For example, based on a survey of 387 online bookstore users, Liang et al. (2012) reported that personalized customer services can generate higher perceived usefulness compared with non-personalized ones. From a mobile location-awareness marketing perspective, Xu et al. (2011) found that personalization approaches and personal characteristics can influence the way individuals calculate the utility gained by disclosing personal information; in other words, personalization can somehow override privacy concerns. Focusing on mobile advertising, a recent study conducted by Sutanto et al. (2013) concluded that personalized and privacy-safe applications engaged in higher levels of application usage behavior. In the current study, we focus on personalized services where the benefits are more apparent to consumers.

Although most of these studies have addressed personalization and privacy issues in the online setting, several of their conclusions could be extended to the mobile arena. Therefore, we have chosen to examine the presence of personalized factors in the usage of mobile services (i.e., perceived benefit and hence willingness to provide information), as well as their direct (i.e., intention to use) and indirect effects (i.e., perceived ease-of-use and perceived usefulness) on a mobile user's decision to use these services.

Hypothesis 3a: The level of personalized service is positively related to mobile user's perceived benefit.

Hypothesis 3b: The level of personalized service is positively related to mobile user's perceived risk.

Hypothesis 3c: The level of personalized service is positively related to mobile user's perceived ease-of-use of a mobile application.

Hypothesis 3d: The level of personalized service is positively related to mobile user's perceived usefulness of a mobile application.

Hypothesis 3e: The level of personalized service is positively related to mobile user's perceived enjoyment of a mobile application.

Hypothesis 3f: The level of personalized service is positively related to mobile user's intention to use a mobile application.

The Effect of Perceived Information Control

When a consumer chooses to enter into a relationship with a company, he or she must first be convinced that it is in their best interest to do so (Chen and Rea Jr, 2004). At the point when a consumer's personal information (e.g., mailing list) is sold to a third party, the relationship between that consumer's original interests and the company's interest changes. In particular, it may become more tenuous. In this case, the consumer may not be interested in the relationship with the third party because they may not share any of the profit from that transaction (Varian, 1996). Nevertheless, from an economic perspective, such costs could be somehow mitigated if the individual has "a voice" in the transaction (Varian, 1996). In other words, if the consumer is able to choose whether or not to sell his or her information to the third party (e.g., the consumer may be interested in selling information to a third party which could then send him/her useful information), they may be less likely to worry about information privacy.

The case mentioned above relates to the avoidance of unwanted persons or contact during an interaction. Goodwin (1991) defined this type of control as "control over unwanted presence in the environment" (p.151). In a consumer context, when individuals provide personal information to a company, people should have the right to know why the information is collected, its expected uses, and any means of reuse elsewhere. However, the unwanted presence of others is not so easy to control. Xu (2010) drew upon a study by Yamaguchi (2001), proposing that consumers be able to exercise personal control or proxy control over their personal information via technology, industry self-regulation and government regulation in a location-based service context. In reality, however, most companies lack privacy policy creation and implementation (Chen and Rea Jr, 2004). As a result, consumers must rely on personal controls. In addition to privacy-enhancing technology, as suggested by Xu (2010), consumers may develop mechanisms to protect their information privacy by directly controlling the flow of their personal information to others. This can take place in three ways (Chen and Rea Jr, 2004): (1) falsification of a user's personal information; (2) passive reaction, by which a user ignores or employs a simple mechanism to block another person's presence; and (3) identity modification, whereby a user alters his or her identifications. It should be noted, however, that all three control techniques would hamper the development of online business. In the present study, we have assumed that users rely on technology solutions, meaning that users have the ability to determine what information to share, with whom they will share it, and how to control its dissemination.

More generally, research has shown that the ability of consumers to take control of their personal data to some extent offsets the risk of possible negative consequences (Dinev & Hart, 2004; Stewart and Segars, 2002). Internet customers tend to think that information disclosure is less invasive, and less likely to lead to negative consequences when they can control when and how their information is disclosed and used in the future (Bandyopadhyay, 2012; Malhotra et al., 2004). Such a belief could

easily extend to customers' attitudes to mobile applications. It is worth noting that here the notion of control includes two different types in the privacy context: control over information disclosure before the information is obtained, and control over information use once the information has been obtained (Dinev et al., 2013). In the current study, we conceptualize information control in a general way, addressing both dimensions with regards to personal information.

In fact, privacy concerns become particularly salient in the mobile context because a mobile phone is rather personal, and could potentially be associated with a consumer's lifestyle habits, behaviors, and movement (King and Jessen, 2010; Xu, 2010). Researches in this domain have also reported similar findings (e.g., Christin et al., 2013). As a consequence, mobile users' perceived risks are likely to be reduced in cases when they believe they have ability to take control of their disclosed personal data. This leads them to disclose more personal information. Therefore we propose the following:

Hypothesis 4a: The level of perceived control ability over mobile user's personal information is negatively related to his/her perceived risk.

Hypothesis 4b: The level of perceived control ability over mobile user's personal information is positively related to his/her willingness to provide information.

Hypothesis 4c: The level of perceived control ability over mobile user's personal information is positively related to his/her intention to use.

Control Variables

To account for other influences on the core dependent variable, we have included a robust set of controls in the research model.

Despite the rapid growth of smartphone use in our society, some people still choose to avoid them because they feel anxious about using mobile technologies. Reflection on the findings of previous studies (Venkatesh, 2000; Simonson et al., 1987), mobile technology anxiety relates to user's general perceptions about the smartphone use, it is a technology-oriented individual difference that provides insight into the impact of consumers' general concerns about mobile technology on information privacy. Wang (2007) defined that mobile computer anxiety as a negative affective response by individuals towards interactions with mobile computers or towards the possibility of using one. Users' mobile technology anxiety can directly influence their intention to use mobile applications. Thus, we have included it as a control variable.

Furthermore, previous studies have shown that personal characteristics, such as personal innovation, are likely to affect mobile application usage level (Xu et al., 2011). Personal innovation refers to the degree to which an individual is receptive to new ideas and new technologies (Venkatesh et al., 2012). When a new application is released, mobile users may use it simply for the novelty value. Thus, we have included it in the research model.

In addition, previous studies (e.g., Chen et al., 2013; Kuo et al. 2007; Nosko et al., 2012) have consistently shown that demographic differences such as gender and age have a strong impact on information privacy concerns. Overall, male consumers exhibit fewer privacy concerns than female consumers when using the Internet to purchase products (Graeff and Harmon, 2002; Wills and Zeljkovic, 2011). Young Internet users tend to have positive views on the collection of personal information for marketing purposes (Gervey and Lin, 2000). Thus, gender and age have also been included in this model.

Theoretical Model

To summarize, all the constructs and related hypotheses are indicated in Figure 2.

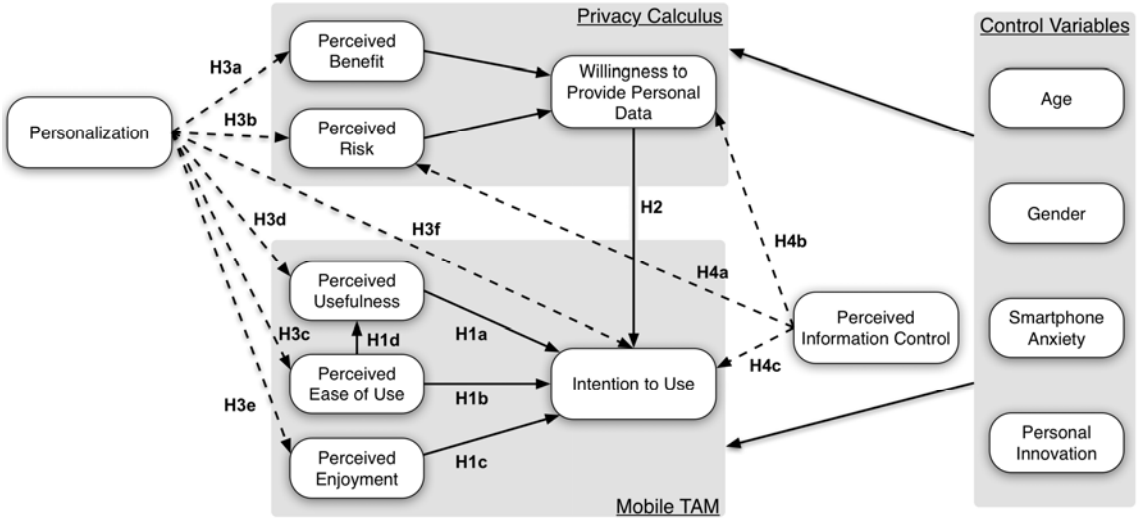

Figure 2. Theoretical model

Methodology

The purpose of this study is to understand the mobile TAM and consumer privacy calculus, taking into consideration perceived information control and personalization. Hence, we have sought to identify the factors that have the greatest explanatory power.

Sample

A total of 308 participants volunteered to participate in the study. As an incentive to participate, volunteers were given an opportunity to enter a lottery to win a Samsung Galaxy S4. In total, 308 people took part in the study: 204 of these were males and 104 were females. All subjects ranged in age between 18 and 58 years, with an average age of 30.8 years. Among the participants, 77.3% indicated that they were familiar with smartphones (score above 4), and 58.5% indicated that they

were familiar with LBS mobile applications (score above 4). Table 1 gives a summary of the demographic characteristics of the respondents.

Table 1. Respondents' demographics (n=308)

	Number	Percentage
Gender		
Male	204	66.2%
Female	104	33.8%
Age		
under 20	32	10.4%
21-25	85	27.6%
26-30	37	12.0%
31-35	50	16.2%
36-40	43	14.0%
41-49	47	15.3%
50 and over	14	4.5%
	Mean	Std.
Familiar with Smartphone	5.5	1.59
Familiar with LBS application	4.5	1.72

Bélanger and Crossler (2011) based their work on a review of 500 papers that examine information privacy research in Information Systems. They argued that studies that rely heavily on student-based samples may result in findings of limited generalizability. The sample of participants does not only focus on students; rather, it also includes diverse profiles of potential users from various occupational fields. Thus, we consider the results of this study to have adequate generalizability.

Measurement

This study primarily used a scenario-based (Appendix A) survey to address the perceptions of mobile users of privacy calculus and their attitude to mobile technology acceptance. The main independent variables in this study are personalization and perceived information control. Thus, we designed 2X2 scenarios and explained how different these four scenarios in the Appendix A: (A) a situation that has both a low level of personalization and perceived information control; (B) a situation that has a high level of personalization but a low level of perceived information control; (C) a situation that has a low level of personalization but a high level of perceived information control; and (D) a situation that has both a high level of personalization and a high level of perceived information control.

The measures used in this study were mainly adapted from relevant prior studies (Davis, 1989; Venkatesh, 2000; Xu et al., 2010; Xu et al., 2011). Willingness to disclose data was assessed by a

single question adapted from Culnan and Armstrong (1999): how likely would you be to provide your personal information (including your location) when using "Check Me In"? Otherwise, multi-item measures were established for the following variables:

- Both Perceived benefits (BENEFIT, 4 items) and Perceived risks (RISK, 3 items) were measured using questions adapted from Xu et al. (2010). Thus we adopted the definition of perceived risks as: "the expectation of losses associated with the release of personal information to the service provider" (p.149)
- Perceived ease-of-use (EASE): was assessed on the basis of four items taken from Venkatesh (2000).
- Perceived enjoyment (ENJOYMENT): was measured using a basis of three items adapted from Venkatesh et al (2012).
- Perceived usefulness (USEFULNESS): we did not adopt the original TAM scales for perceived usefulness as in our case "improved job performance", for instance, might be an inappropriate outcome of using the social mobile application. For this reason, we developed new items that preserve the utilitarian nature of the scale.
- Intention to use (INTENTION): was measured by 4 items, of which 2 items were taken and adapted from Venkatesh (2000). The other 2 new items were developed specially for this study.
- Personal innovation (INNOVATION): was assessed using three items taken from Xu et al. (2011).
- Smartphone anxiety (ANXIETY): was based on six items taken from a study by Venkatesh (2000). The original measure was computer anxiety. To meet the required thresholds, we had to delete "it would not bother me to take smartphone courses", a factor loading analysis that was revealed during our study.
- Multi-item measures (7-Likert scale) were established for most of the measures except for user's willingness to disclose data. The items for all the measures are listed in the Appendix B.

Procedure

The initial questionnaire was reviewed by two experts: one male from an information system background and one female from a marketing background. It was then distributed to 10 mobile users who were familiar with smartphone and social applications. These two pilot studies have two objectives: first, to clarify the scenarios described and the questions included in the survey; and second, to ensure that the experiment is well planned and effectively executed. An analysis of their feedback revealed that the respondents found some descriptions in the scenarios were unnecessary; these were removed, and several revisions to items on the questionnaire were made.

Each participant was asked to answer the questionnaire with LimeSurvey online. All participants were told that there were no right or wrong answers. The response time was recorded. It took an

average of 15-20 minutes to complete, including reading the survey instructions, the scenarios, and completion of the questions.

The final survey comprised three parts: (1) socio-demographic characteristics, to measure age, gender, and country of the origin; (2) a general question, to measure subjects' privacy concerns, technology anxiety and innovation, and their knowledge of smartphone and location-based mobile applications; and (3) a description of a scenario and questions based on the scenario, which formed the main body of this study and were designed to measure key variables in the model.

With a few exceptions, respondents were asked to use a seven-point scale, from 1 (strongly disagree) to 7 (strongly agree) to describe their perceptions regarding a statement of the relevant variable. In order to minimize possible ordering effects of questions to subjects, some questions were reverse scored and questions in scenarios were randomly ordered.

Experimental manipulations were checked in two stages. First, we discounted data from participants who spent less than 10 seconds on reading the scenario descriptions. Second, at the end of the questionnaire, respondents were asked to state the name of the mobile application for manipulation check purposes. Of the 340 total questionnaires, 32 were removed from the final sample, as they failed to answer this question. These manipulation checks resulted in a final sample of 308 usable and valid responses.

Results

The reliability of each multi-item measure was assessed by calculating Cronbach's coefficient alpha. Cronbach's alpha and descriptive statistics for the key constructs used in the research model are presented in Table 2 and Table 3, which contain information on the correlation coefficients between all constructs. Table 3 indicated that the variable perceived benefits and perceived usefulness are highly correlated (0.840, $p<0.01$). The reason is probably because both variables describe values to users. However, there exist differences between the two constructs. Perceived benefits refer to direct or indirect advantages that mobile users can enjoy by using a specific mobile application. For example, users can benefit from a wider range of monitory benefits (e.g., discount), increased sociality and so forth. Perceived usefulness, on the other hand, discusses about the functions and utility of a mobile application. Moreover, in our framework these two variables are in two separated models where there are no direct relationships between them. Therefore we believe it would not affect the validity of our results.

Table 2. Descriptive statistics for the constructs (n=308)

Variables	Number of Items	Reliability (Cronbach's alpha)	Mean (Value range 1-7)	Std.
Perceived benefits (BENEFIT)	4	0.854	4.806	1.186
Perceived risks (RISK)	3	0.863	4.487	1.472
Perceived ease-of-use (EASE)	4	0.801	4.868	1.029
Perceived usefulness (USEFULNESS)	3	0.841	4.618	1.349
Perceived enjoyment (ENJOYMENT)	3	0.866	4.568	1.217
Intention to use (INTENTION)	4	0.917	4.677	1.367
Personal innovation (INNOVATION)	3	0.910	4.568	1.546
Smartphone anxiety (ANXIETY)	5	0.879	2.363	1.152

Table 3. Pearson correlations between constructs (n=308)

Variables	01	02	03	04	05	06	07	08	09
01 Personalization (PERS)	1								
02 Perceived information control (CONTROL)	0.006	1							
03 Perceived benefits (BENEFIT)	0.193**	0.023	1						
04 Perceived risks (RISK)	0.113*	-0.394***	0.063	1					
05 Willingess to disclose data (WILLINGNESS)	0.108	0.266***	0.516***	-0.372***	1				
06 Perceived ease-of-use (EASE)	0.147***	0.035	0.617***	0.118**	0.356***	1			
07 Perceived usefulness (USEFULNESS)	0.215***	0.025	0.840***	0.018	0.574***	0.631***	1		
08 Perceived enjoyment (ENJOYMENT)	0.110	0.087	0.538***	-0.115**	0.442***	0.393***	0.570***	1	
09 Intention to use (INTENTION)	0.146**	0.200***	0.648***	-0.272***	0.614***	0.539***	0.749***	0.693***	1

After establishing the validity of the measures, we tested our hypotheses by examining the sign and significance of the path coefficient. Each hypothesis was tested based on the sign and the statistical significance for its corresponding path in the structural model.

Privacy Calculus in Mobile Context

To verify privacy calculus in a mobile context, we first conducted a simple regression analysis with the continuous variable – willingness to disclose data (WILLINGNESS) as the dependent variable and perceived benefit (BENEFIT) and perceived risks (RISK) as the independent variables. We then introduced the two manipulated variables, personalization (PERS) and perceived information control (CONTROL), in the model. These two variables were coded as dichotomous variables with 1 being with condition and 0 being without condition. In step 3, our analysis also included control variables: AGE, GENDER, personal innovation (INNOVATION) and smartphone anxiety (ANXIETY). The results are given in Table 4.

Table 4. Regression results of privacy calculus

Depedent variable: WILLINGNESS			
Predictor variable	STEP1	STEP2	STEP3
Intercept	1.386***	0.971**	1.280*
BENEFIT	0.887***	0.864***	0.801***
RISK	-0.535***	-0.484***	-0.474***
PERS		0.182	0.158
CONTROL		0.420**	0.362*
AGE			0.008
GENDER			0.115
INNOVATION			0.008
ANXIETY			-0.198**
F-value	169.68	90.94	50.22
R^2	0.431	0.443	0.454

As seen in Table 4, all three regression models were statistically significant at the $p<0.01$ level. In step 1, the overall regression model with the two predictor variables was found to be statistically significant: $F(2, 305) = 169.68$, with $R^2 = 0.431$. Both predictor variables were found to significantly affect users' willingness to disclose personal data. This result is consistent with previous findings on privacy calculus (e.g., Dinev and Hart, 2006a). In step 2, the overall regression model with the two predictor variables was found to be statistically significant: $F(4, 303) = 90.94$, with $R^2 = 0.443$. Interestingly, users' perceived information control was found to have a significantly positive effect on users' willingness to disclose data (standardized coefficient estimate = 0.420, $p<0.01$), whereas personalization has no significant influence on users' willingness to disclose data. Thus, H4b was supported. Step 3 concluded other control variables and the intercept coefficient in this model was found to be less significant because some of the effects were explained by users' background information (e.g., anxiety).

We conducted a further analysis to address the effect of personalization (PERS) and perceived information control (CONTROL) on predictor variables in the framework of the privacy calculus. Here, perceived benefit (BENEFIT) and perceived risk (RISK) were treated as dependent variables. We also included control variables in our analysis. Both regression models came out to be statistically significant at the $p<0.01$ level, $F(6, 301) = 8.15$ and $F(6, 301) = 14.43$. The R^2 obtained were 0.174 and 0.193 respectively. Personalization was positively related to the perceived benefit (standardized coefficient estimate = 0.419, $p<0.01$) and perceived risk (standardized coefficient estimate = 0.362, $p<0.05$). Therefore both H3a and H3b were both supported. Perceived information control, on the other hand, had a strong negative impact on perceived risk (standardized coefficient estimate = -1.071, $p<0.01$), but had no significant effect on perceived benefit (standardized coefficient estimate = -0.050, n.s.). Hence, we found support for H4a. The results are given in Table 5.

Table 5. Regression results predicting BENEFIT and RISK

	Regression model 1	Regression model 2
Dependent variables:	BENEFIT	RISK
Intercept	4.159***	3.478***
PERS	0.419***	0.362**
CONTROL	-0.050	-1.071***
AGE	0.002	0.013
GENDER	0.426***	0.242
INNOVATION	0.113***	0.083
ANXIETY	-0.274***	0.130*
F-value	8.15	14.43
R^2	0.174	0.193

TAM in Mobile Context

A maximum likelihood structural equation modeling was used to test the mobile TAM. Figure 3 and Figure 4 depict the results of set 1 of the proposed hypotheses and of a final, adjusted mobile TAM with standardized coefficients. In the hypothesis, perceived ease-of-use had a direct effect on users' intentions to use mobile applications, whilst perceived enjoyment only had a direct impact on users' intentions to use mobile applications. In the final model (CFI=0.949), however, perceived ease-of-use served as a mediator for the influence of perceived usefulness and perceived enjoyment on users' intentions to use mobile applications. Thus, against our expectations, H1b was not supported. This finding is of particular interest because perceived ease-of-use has served as a key element since the integration of the TAM theory. This has been proved by many prior studies (e.g., Venkatesh, 2000; Venkatesh and Davis, 2000). Furthermore, perceived enjoyment not only had a direct impact (standardized coefficient estimate = 0.377, $p<0.01$), but also had an indirect impact (via perceived usefulness, standardized coefficient estimate = 0.354, $p<0.01$) on users' intentions to use mobile applications. Obviously, perceived enjoyment has replaced the role of perceived ease-of-use, and has become an important predictor in mobile users' intentions to use mobile applications. Among all predictor variables, perceived usefulness still had the strongest effect on users' intentions to use mobile applications (standardized coefficient estimate = 0.619, $p<0.01$). Therefore, H1a, H1c and H1d were all supported.

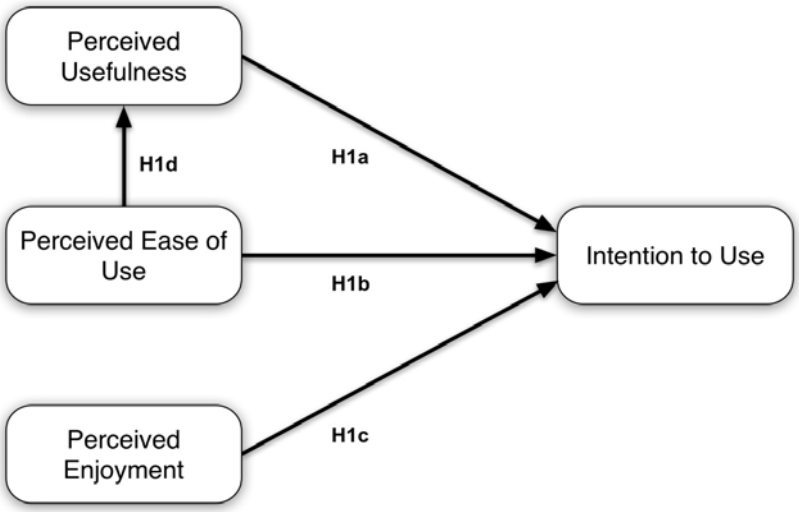

Figure 3. Proposed mobile TAM (Hypothesis set 1)

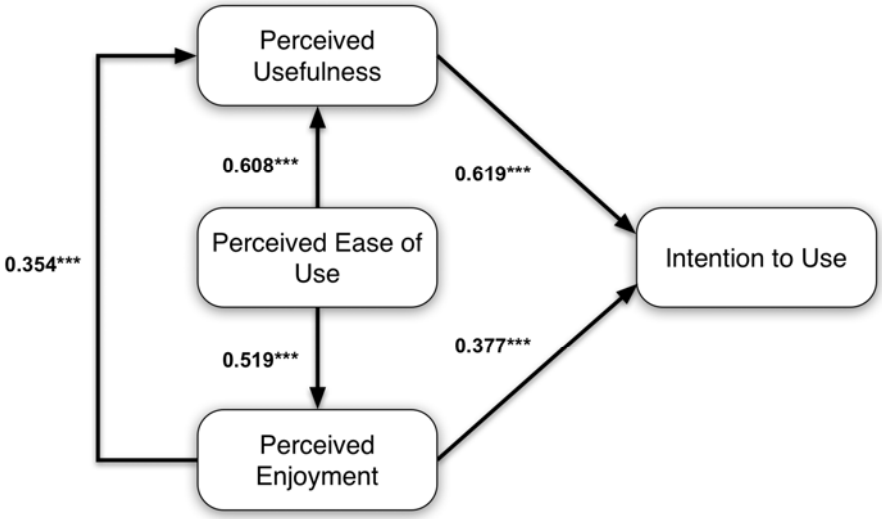

Figure 4. Final mobile TAM

To test H2, we added a privacy calculus in the final mobile TAM and found that users' willingness to disclose data was positively related to users' intentions to use mobile applications (standardized coefficient estimate = 0.011, $p<0.01$). Hence, H2 was also supported.

Next, we conducted a regression analysis in three steps to examine the effect of personalization and perceived information control. Here, users' intentions to use mobile applications (INTENTION) were the dependent variable. Again, the first step contained three main predictor variables: perceived usefulness (USEFUL), perceived ease-of-use (EASE) and perceived enjoyment (ENJOYMENT); the second step added personalization characteristics (PERS) and users' perceived information control (CONTROL). The third step included all four control variables. Table 6 shows the regression results.

Table 6. Regression results of TAM

Depedent variable: INTENTION			
Predictor variable	STEP1	STEP2	STEP3
Intercept	-0.101	-0.245	0.247
USEFUL	0.477***	0.488***	0.485***
EASE	0.119*	0.114*	0.099
ENJOYMENT	0.437***	0.418***	0.418***
PERS		-0.032	-0.023
CONTROL		0.418***	0.391***
AGE			-0.009*
GENDER			0.007
INNOVATION			-0.011
ANXIETY			-0.033
F-value	182.61	151.51	91.26
R^2	0.67	0.694	0.699

All three regression models were found to be statistically significant. In the absence of other variables (step1), F (2, 305) = 182.61, with R^2 = 0.670. Here, perceived ease-of-use had a marginally significant effect on users' intentions to use mobile applications (standardized coefficient estimate = 0.119, p<0.1). In step 2, F (4, 303) = 151.51, with R^2 = 0.694. CONTROL was found to be positively related to users' intentions to use mobile applications (standardized coefficient estimate = 0.418, p<0.01). Thus, we found support for H4c.The results for the effect of PERS on users' intentions to use mobile applications were surprising. We found no relationship between them (standardized coefficient estimate = -0.032, n.s.); thus, we failed to provide evidence for H3f. In Step 3, where all control variables were included, F (6, 301) = 91.26, and R^2 value increased to 0.699. We obtained similar results for PERS and CONTROL, but perceived ease-of-use no longer had a strong effect on users' intentions to use mobile applications (standardized coefficient estimate = 0.099, n.s.).

In order to test H3c, H3d and H3e, we conducted three simple regression models. As seen in Table 7, the first regression model was found to be statistically significant: F (8, 299) = 68.15, with R^2 = 0.552. Personalized services had a strong impact on perceived usefulness (standardized coefficient estimate = 0.270, p<0.01). Thus, we found evidence to support H3d. The second regression model was also statistically significant: F (6, 301) = 17.50, with R^2 = 0.224. As hypothesized in H3c, perceived ease-of-use was positively related to personalized services (standardized coefficient estimate = 0.315, p<0.01). Similarly, we found partial support for H3e, which hypothesized that perceived enjoyment was positively related to personalized services (standardized coefficient estimate = 0.101, p<0.1), although the R^2 was a bit lower (0.172) in regression model 3.

Table 7. Regression results predicting USEFUL, EASE and ENJOYMENT

	Regression model 1	Regression model 2	Regression model 3
Dependent variables:	USEFUL	EASE	ENJOYMENT
Intercept	-0.411	3.556***	2.491***
EASE	0.561***	-	0.471***
ENJOYMENT	0.408***	-	-
PERS	0.270**	0.315***	0.101*
CONTROL	-0.095	0.027	0.150
AGE	0.005	-0.001	-0.001
GENDER	0.328***	0.395***	0.095
INNOVATION	0.008	0.225***	0.071
ANXIETY	-0.114**	-0.147**	-0.052
F-value	68.15	17.50	2.59
R^2	0.552	0.224	0.172

Discussion

Discussion of the Findings

The overall goal of this study is to examine the relationships between beliefs about information privacy (privacy calculus) and mobile application usage intentions (e.g., TAM). A further goal is to shed light on the effects of personalization and the ability of users to maintain control over their personal data in a mobile context. We integrated privacy calculus theory into the mobile TAM framework to form the theoretical foundation for this study. In this way, this study was able to conceptualize and empirically test the effect of personalized services and the ability of users to maintain control over their personal data in terms of privacy concerns relating to mobile applications.

In general, the results of both the hierarchical regression analysis and structural equation analysis provide strong support for the proposed research model. The detailed results of the tests of our hypotheses are summarized in Table 8.

Table 8. Summary of results of the tests of hypotheses

	Hypotheses	Result
H1a	USEFUL → + INTENTION	Supported
H1b	EASE → + INTENTION	Not supported
H1c	ENJOYMENT → + INTENTION	Supported
H1d	EASE → + USEFUL	Supported
H2	WILLINENESS → + INTENTION	Supported
H3a	PERS → + BENEFIT	Supported
H3b	PERS → + RISK	Supported
H3c	PERS → + EASE	Supported
H3d	PERS → + USEFUL	Supported
H3e	PERS → + ENJOYMENT	Supported
H3f	PERS → + INTENTION	Not supported
H4a	CONTROL → - RISK	Supported
H4b	CONTROL → + WILLINGNGESS	Supported
H4c	CONTROL → + INTENTION	Supported

As presented in the results, the most striking finding was that perceived enjoyment had replaced the role of perceived ease-of-use in a traditional technology acceptance situation. This had a strong effect on users' intentions to use mobile applications, indicating that a hedonic element is a key component in a mobile context. The structural equation analysis also suggested that the link between perceived usefulness and users' intentions to use mobile applications is stronger than for other direct and indirect effects. This result confirmed prior TAM research which showed that perceived usefulness was a more important predictor of intended system usage than others (Davis, 1989). Perceived usefulness also mediated the relationship between perceived ease-of-use and perceived enjoyment in a mobile context. In terms of the TAM framework, however, we did not find that perceived ease-of-use of mobile applications had a direct impact. One possible reason is that, in a mobile context, such an effect is offset, to some extent, by enjoyment and usefulness.

Another surprising outcome of this study is that our results failed to support the hypothesis that personalized services directly affect users' intentions to use mobile applications (H3f). While offering a personalized service had a strong impact on both perceived enjoyment and perceived usefulness, it had no direct impact on whether or not users would like to use a specific application. This might imply that mobile users are more aware of the existence of potential benefits, such as enjoyment and usefulness. In addition, we have proved that personalized services would increase user's perceived risk, which had a negative effect on their willingness to provide personal data. It hence in turn decreased mobile user's intention to use mobile application. To some extent, this negative effect might offset some of the positive effects that come from increased enjoyment and usefulness, resulting in the impact of personalized services on usage intention unclear.

Unlike previous findings on gender difference in privacy issues, we found that females were more likely to value a higher level of perceived benefit, perceived usefulness and perceived ease-of-use compared with male mobile users. In all likelihood, female mobile users are more interested in using social mobile applications and are more likely to enjoy the potential discounts offered by "Check Me In".

Contribution and Implications

This study is a rich source of theoretical implications. First, while prior studies have examined privacy calculus and TAM separately, this paper studies both theoretical models at the same time. We found that users' willingness to disclose data was positively related to users' intentions to use mobile applications. Future research should apply this framework in order to investigate the relationship between users' beliefs and rights, and disclosure behavior regarding privacy issues in general.

Second, this study provides preliminary theoretical insights and empirical evidence into the structural relationships of antecedents that affect mobile users' intention to use applications. Thus, it has extended the understanding of a mobile TAM. Our findings have also proved that the conventional TAM proposed by Davis (1989) no longer fits well in the mobile context. As discussed earlier, perceived ease-of-use did not have a significant impact on users' intention to use mobile applications. Instead, perceived usefulness served fully as a mediator for the influence of perceived ease-of-use on users' intention to use mobile applications. On the other hand, as a new characteristic, perceived enjoyment played an important role (path coefficient is 0.464). In this respect, it can be seen to be similar to perceived usefulness (path coefficient is 0.671). This has important implications for theoretical development. This study serves as a starting point for future research into a mobile TAM, identifying considerable opportunities and opening up new avenues for exploring predictors using a mobile TAM theory.

Third, this study serves as an initial examination of issues relating to privacy by investigating whether or not personalized services and users' ability to control their information can influence personal information disclosure and use intention. Using a privacy calculus lens, we argued that personalized services and perceived information control play an important role in the way that individuals weigh up the utility gained by disclosing personal information against the disutility of adverse effects resulting from such an action. The results also suggest that personalized services can somehow increase users' perceived risks (the path coefficient is 0.362). However, the way that mobile users' value personalization (e.g., its effects on a perceived benefit) was more influential than their concern for potential risks (path coefficient 0.419 versus 0.362). Moreover, this research also builds on previous studies that have sought to understand the effects of users' ability to control information. It provides empirical evidence that perceived information control is an important driver of mobile users' perceived risks, which in turn influences users' willingness to disclose personal information

Another theoretical implication is that whilst the bulk of previous research has examined individuals' willingness to share information and consumer disclosure behavior in either an offline or online setting, this paper contributes empirical results from a mobile context. Our findings support the premise that personal information disclosure involves a cost-benefit trade-off analysis in a mobile privacy calculus. It reveals that perceived benefit was a much stronger predictor than the negative effect of perceived risk. This indicates that when the level of benefit is high, users may not worry too much about any potential risks. Thus, they may be more willing to disclose their personal data in order to use mobile applications.

From the perspective of practice, our findings also provide several important implications for various players. First, the results indicate that mobile users are concerned about their private personal information and are less willing to disclose personal information in m-commerce. These negative consequences could be alleviated by increasing the level of control that users have over disclosed information. Thus, marketers in an m-commerce setting will need to ensure that users are able to control information (e.g., by issuing a privacy statement). Giving users greater perceived information control can reduce users' perceived risk of using mobile applications, which, in turn, can increase their intention to use these applications.

For application designers, this study provides practical guidance as to how to design and develop mobile applications. A simple and enjoyable application will probably encourage more mobile users to download and use that application. In addition, our findings suggest that every new personalization is likely to increase users' anxieties about the risks with providing personal data. Application designers should, therefore, pay careful attention to the relationship between the potential benefits of personalized services to users, and the related privacy problems they may cause.

Limitations

We acknowledge that, like other studies, this paper has its limitations. First, this study has focused on a single mobile application: a geographical location-based social network. If consumers are not interested in connecting with friends through mobile technology, or getting discounts from restaurants and bars, then this application is not going to be of interest to them. Thus, the findings obtained from this study might not be generalizable to other mobile applications (e.g., games).

Second, we admit that an experimental method was used for data collection. Thus, the participants did not use the mobile application in a real-world setting. Experiment based on real users may have an effect on our results.

Finally, despite the care we took in designing the experiment, some common method bias was not avoidable. Although the final sample consisted of people from diverse occupational backgrounds and different age groups, we have to admit that they were mainly from only two countries: China and Switzerland. This may also negatively affect the generalizability of the results. Future research is

needed to address the potential moderate effects of cultures and institutional factors such as regulatory structure.

Conclusion

Building upon the privacy concern literature juxtaposed with the technology acceptance model, this study has developed a theoretical framework that combines the role of personalized services and users' perceived information control in the mobile application context. An interesting finding of this study is that perceived enjoyment has replaced perceived ease-of-use as a main predictor of perceived behavioral intentions in m-commerce. Perceived usefulness still has the strongest impact. At the same time, the results also reveal that users' perceived information control and personalized services has a strong effect on both a privacy calculus and mobile TAM. Marketers and application designers need to understand these influences and address them appropriately to encourage mobile users to disclose personal information and use mobile applications.

References

Ackerman, M. S. (2004). Privacy in pervasive environment: next generation labeling protocols. *Personal and Ubiquitous Computing, 8*, 430-439.

Ackerman, M. S., Cranor, L., & Reagle, J. (1999). Privacy in e-commerce: examining user scenarios and privacy preference. *In Proceeding of ACM conference on electronic commerce*, Denver, Colorado, 1-8.

Adams, D. A., Nelson, R. R., & Todd, P. A. (1992). Perceived usefulness, ease of use, and usage of information technology: a replication. *Management Information Systems Quarterly, 16*, 227-247.

Anderson, C. L., & Agarwal, R. (2011). The digitization of healthcare: boundary risks, emotion, and consumer willingness to disclose personal health information. *Information Systems Research, 22*(3), 469-490.

Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. *Management Information Systems Quarterly, 30*(1), 13-28.

Bandyopadhyay, S. (2012). Consumers' online privacy concerns: causes and effects. *Innovative Marketing, 8*(3), 32-39.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information system. *Management Information Systems Quarterly, 35*(4), 1017-1041.

Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: an empirical examination of the online consumer's dilemma. *Information Technology and Management, 6*, 181-202.

Chen, X., Ma, J., Jin, J., & Fosh, P. (2013). Information privacy, gender differences, and intrinsic motivation in the workplace. *International Journal of Information Management, 33*, 917-926.

Chen, K., & Rea Jr, A. (2004). Protecting personal information online: A survey of user privacy concerns and control techniques. *Journal of Computer Information System, 44*(4), 85-92.

Chorppath, A. K., & Alpcan, T. (2013). Trading privacy with incentives in mobile commerce: a game theoretic approach. *Pervasive and Mobile Computing, 9*, 598-612.

Christin, D., Lopey, P. S., Reinhardt, A., Hollick, M., & Kauer, M. (2013). Share with strangers: privacy bubbles as user-centered privacy control for mobile content sharing applications. *Information Security Technical Report, 17*, 105-116.

Clarke, R. (1999). Internet privacy concerns confirm the case for intervenion. *Communication of the ACM*, *42*(2), 28-31.
Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness and impersonal trust: an empirical investigation. *Organization Science, 10*(1), 104-115.
Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *Management Information Systems Quarterly, 13*(3), 319-340.
Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User aceptance of computer technology: a comparison of two theoretical models. *Management Science, 35*(8), 982-1003.
Dey, A. K., & Abowd, G. D. (2000). Towards a better understanding of context and context-awareness. *In Proceedings of the CHI 2000 Workshop on The What, Who, Where, When, and How of Context-Awareness*, The Hague, Sunderland, United Kingdom.
Dhar, S., & Varshney, U. (2011). Challenges and business models for mobile location-based services and advertising. *Communication of the ACM, 54*(5), 121-129.
Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents – measurement validity and a regression model. *Behavior & Information Technology, 23*(6), 413-422.
Dinev, T., & Hart, P. (2006a). An extended privacy calculus model for e-commerce transactions. *Information System Research, 17*(1), 61-80.
Dinev, T., & Hart, P. (2006b). Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce, 10*(2), 7-29.
Dinev, T., & Hart, P. (2007). Privacy concerns and levels if information exchange: an empirical investigation of intended e-service use. *e-Service Journal, 4*(3), 25-61.
Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts. European Journal of Information System, 22, 295-316.
Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: an integrated model. *Management Information Systems Quarterly, 27*(1), 51-90.
George, J. F. (2004). The theory of planned behavior and internet purchasing. *Internet Research, 14*(3), 198-212.
Gervey, B., & Lin, J. (2000). Obstacles on the internet: a new advertising age survey finds privacy and security concerns are blocking the growth of e-commerce. *Advertising Age, 71*(16), 13-22.
Goodwin, C. (1991). Privacy: recognition of a consumer right. *Journal of Public Policy and Marketing, 10*(1), 149-166.
Graeff, T. R., & Harmon, S. (2002). Collecting and using personal data: consumers' awareness and concerns. *Journal of Consumer Marketing, 19*(4), 302-318.
Hann, I. H., Hui, K. L., Lee. T. S., & Png, I. P. L. (2002). Online information privacy: measuring the cost-benefit trade-off. *In Proceeding of 23rd International Conference on Information System*, Barcelona, Spain, 1-10.
Hong, W., & Thong, J. Y. L. (2013). Internet privacy Concerns: An Integrated Conceptualization and Four Empirical Studies. *Management Information Systems Quarterly, 37*(1), 275-298.
Junglas, I. A., Johnson, N. A., & Spitzmuller, C. (2008). Personality traits and concern for privacy: an empirical study in the context of location-based services. *European Journal of Information Systems, 17*(4), 387-402.
Junglas, I. A., & Watson, R. T. (2008). Location-based services. *Communications of the ACM, 51*(3), 65-69. doi:10.1145/1325555.1325568
Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., & Greer, C. (2013). Information disclosure on mobile devices: re-examining privacy calculus with actual user behavior. *International Journal of Human Computer Studies, 71*, 1163-1173.
Kim, E., & Lee, B. (2009). E-service quality competition through personalization under consumer privacy concerns. *Electronic Commerce Research and Applications, 8*, 182-190.
King, N. J., & Jessen, P. W. (2010). Profiling the mobile consumer – privacy concerns when behevioural advertisers target mobile phones – Part I. *Computer Law and Security Review, 26*, 455-478.

Kuo, F. Y., Lin, C. S., & Hsu, M. H. (2007). Assessing gender differences in computer professionals' self-regulatory efficacy concerning information privacy practices. *Journal of Business Ethics, 73*, 145-460.

Liang, T. P., Chen, H. Y., Du, T., Turban, E., & Li, Y. (2012). Effect of personalization on the perceived usefulness of online customer services: a dual-core theory. *Journal of Electronic Commerce Research, 13*(4), 275-288.

Liu, Z., Bonazzi, R., Fritscher, B., & Pigneur, Y. (2011). Privacy-friendly business models for location-based mobile services. *Journal of theoretical and applied electronic commerce research*, *6*(2), 90-107.

Liu, Z., Shan, J., Bonazzi, R., & Pigneur, Y. (2014). Privacy as a tradeoff: introducing the notion of privacy calculus for context-aware mobile applications. *In Proceeding of the 47st Hawaii International Conference in System Sciences*, Waikoloa, Hawaii, USA, 1063-1072.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336-355.

Nam, C., Song, C., Lee, E., & Park, C. I. (2006). Consumers' privacy concerns and willingness to provide marketing-related personal information online. *Advances in Consumer Research, 33*, 212-217.

Nosko, A., Wood E., Kenney, M., Archer, K., De Pasquale, D., Molema, S., & Zivcakova, L. (2012). Examining priming and gender as a means to reduce risk in a social networking context: can stories change disclosure and privacy setting use when personal profiles are constructed? *Computers in Human Behavior, 28*, 2067-2074.

Phelps, J., Nowak, G., & Ferrell, E. (2000). privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy and Marketing, 19*(1), 27-41.

Pomery, E. A., Gibbons, F. X., Reis-Bergan, M., & Gerrard, M. (2009). From willingness to intention: Experience moderates the shift from reactive to reasoned behavior. *Personality and Social Psychology Bulletin, 35*(7), 894-908.

Sheng, H., Nah, F.F. H., & Siau, K. (2008). An experimental study on ubiquitous commerce adoption: impact of personalization and privacy concerns. *Journal of the Association for Information Systems, 9*(6), 344–376.

Simonson, M. R., Maurer, M., Montag-Torardi, M., & Whitaker, M. (1987). Development of a standardized test of computer literacy and a computer anxiety index. *Journal of educational computing research*, *3*(2), 231-247.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: measuring individual's concerns about organizational practices. *Management Information Systems Quarterly, 20*(2), 167-196.

Spiekermann, S., Grossklags, J., & Berendt, B. (2001). E-Privacy in 2nd generation e-commerce: privacy preferences versus actual behavior. *In Proceedings of ACM conference in electronic commerce*, Tampa, Florida, US, 38-46.

Stewart, K. A., & Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. *Information Systems Research, 13*(1), 36-49.

Sutanto, J., Palme, E., Tan, C. H., & Phang, C. W. (2013). Addressing the personalization-privacy paradox: an empirical assessment from a field experiment on smartphone users. *Management Information Systems Quarterly, 37*(4), 1141-1164.

Tam, K. Y., & Ho, S. Y. (2006). Understanding the impact of web personalization on user information processing and decision outcomes. *Management Information Systems Quarterly, 30*(4), 865-890.

Van der Heijden, H. (2004). User acceptence of hedonic information system. *Management Information Systems Quarterly, 28*(4), 695-704.

Varian, H. R. (1996). Economic aspects of personal privacy. Technical report, University of California, Berkeley, US.

Venkatesh, V. (2000). Determinants of perceived ease of use: integrating control, intrinsic motivation, and emotion into the technology acceptance model. *Information System Research. 11*, 342-365.

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: four longitudinal field studies. *Management Science, 46*(2), 186–204.

Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. *Management Information Systems Quarterly, 36*(1), 157-178.

Wang, Y. S. (2007). Development and validation of a mobile computer anxiety scale. *British Journal of Educational Technology*, *38*(6), 990-1009.

Wills, C. E., & Zeljkovic, M. (2011). A personalized approach to web privacy: awareness, attitudes, and actions. *Information Management and Computer Security, 19*(1), 53-73.

Xu, J. D., Benbasat, I., & Cenfetelli, R. T. (2013). Integrating service quality with system and information quality: an empirical test in the e-service context. *Management Information Systems Quarterly, 37*(3), 777-794.

Xu, H. (2010). Locus of Control and Location Privacy: An empirical study in Singapore. *Journal of Global Information Technology Management, 13*(3), 63-87.

Xu, H., Teo, H. H., Tan, B. C. Y., & Agarwal, R. (2010). The role of push-pull technology in privacy calculus: the case of location-based services. *Journal of Management Information Systems, 26*(3), 135-173.

Xu, H., Luo, X. R., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems, 51*(1), 42-52. doi:10.1016/j.dss.2010.11.017

Yamaguchi, S. (2001). Culture and control orientations. In:D. Matsumoto (Ed.), The handbook of culture and psychology (pp.223-243). Oxford, United Kingdom: Oxford University Press.

APPENDIX A: Scenarios

Basic scenario :

Assume that you have installed a new application called “Check Me In” on your mobile phone. It is a geographical location based social network that allows you to post your location at a restaurant or a bar (“checking in”) and connect with your friends.

You can now see where your friends check in, explore restaurants you haven't yet visited and monitor popular destinations. Moreover, points and badges are awarded for checking in at various restaurants. For example, if you have checked in a certain restaurant for the first time, you will earn a “newbie” badge. If you have checked in a certain amount of times in a given period at a certain restaurant, you will be honored as “VIP”. Special deals (e.g., a free drink or 10% discount of the meal) from that restaurant will be offered to you.

Scenario A (both low level of personalization and perceived information control): basic scenario with the following texts

In addition, you can search for particular menu items in a certain place. When you are searching for a specific type of restaurants in your city, this application will suggest you some venues in the same category **randomly** nearby.

Your personal information, including your name, email address, phone number, birthday, use information regarding your use of this application, and browser information will be collected by this application. **We may draw upon** this information in order to research the effectiveness of the services, adapt the service of the community to your needs, and develop new features. In addition, **restaurants you visited may have greater access to the record of your visit**.

Scenario B (high level of personalization, and low level of perceived information control): basic scenario with the following texts

In addition, you can search for a specific type of restaurants in your city. This application will provide you with tailored suggestions **based on your friends’ previous “check-ins”** nearby. For example, you may want to try a restaurant where your friends have been for many times and have good reviews from them. You may also want to go with your friends to a restaurant where your friends are honored as “VIP”.

Your personal information, including your name, email address, phone number, birthday, use information regarding your use of this application, and browser information will be collected by this application. **We may draw upon** this information in order to research the effectiveness of the services, adapt the service of the community to your needs, and develop new features. In addition, **restaurants you visited may have greater access to the record of your visit**.

Scenario C (low level of personalization, and high level of perceived information control): basic scenario with the following texts

In addition, you can search for particular menu items in a certain place. When you are searching for a specific type of restaurants in your city, this application will suggest you some venues in the same category **randomly** nearby.

Your personal information, including your name, email address, phone number, birthday, use information regarding your use of this application, and browser information will be collected by this application. However, such information **will not be used by any means without your permission**. Such usage includes activities for the purpose of researching the effectiveness of the services, adapting the service of the community to your needs, and developing new features, with or without any third party (e.g., restaurants).

Scenario D (both high level of personalization and perceived information control): basic scenario with the following texts

In addition, you can search for a specific type of restaurants in your city. This application will provide you with tailored suggestions **based on your friends' previous "check-ins"** nearby. For example, you may want to try a restaurant where your friends have been for many times and have good reviews from them. You may also want to go with your friends to a restaurant where your friends are honored as "VIP".

Your personal information, including your name, email address, phone number, birthday, use information regarding your use of this application, and browser information will be collected by this application. However, such information **will not be used by any means without your permission**. Such usage includes activities for the purpose of researching the effectiveness of the services, adapting the service of the community to your needs, and developing new features, with or without any third party (e.g., restaurants).

APPENDIX B: Measure Items

Smartphone Anxiety (ANXIETY) was based on items taken from a study by Venkatesh (2000):

Concerning smartphone …

…it does not scare me at all.

…working with it makes me nervous.

…it makes me feel uneasy.

…it makes me feel uncomfortable.

…I get a sinking feeling when I think of trying to use it.

Personal innovation (INNOVATION) was assessed using three items taken from Xu et al. (2011):

Concerning new information technology …

…once I heard about it, I would look for ways to experiment with it.

…among my peers, I am usually the first to try out new information technologies.

… I like to experiment with new information technologies.

Perceived benefits (BENEFIT) was measured using questions adapted from Xu et al. (2010):

Overall, I fell that using "Check Me In" is beneficial.

"Check Me In" allows me to see where my friends like to go.

Using "Check Me In" would give me special deals in a restaurant or a bar.

"Check Me In" allows me to record and share my adventures.

Perceived risks (RISK) was measured using questions adapted from Xu et al. (2010):

There would be high potential for loss in disclosing my personal information to "Check Me In".

It would be risky to disclose my personal information to "Check Me In".

Providing "Check Me In" with my personal information would involve many unexpected problems.

Perceived ease-of-use (EASE) was assessed on the basis of four items taken from Venkatesh (2000):

Learning to operate "Check Me In" would be easy for me.

I find it easy to get "Check Me In" to do what I want it to do.

I find "Check Me In" to be easy to use.

My interaction with "Check Me In" is clear and understandable.

Perceived enjoyment (ENJOYMENT) was measured using a basis of three items adapted from Venkatesh et al (2012):

Using "Check Me In" would be fun.

Using "Check Me In" would be enjoyable.

Using "Check Me In" would be very entertaining.

Perceived usefulness (USEFULNESS) was developed for this study:

I find "Check Me In" to be useful in my daily life.

Using "Check Me In" would always give me good suggestions for a nice restaurant.

Using "Check Me In" would help me to connect with my friends.

Intention to use (INTENTION) was measured and adapted from Venkatesh (2000):

If "Check Me In" is available on Mobile App Store, I predict that I will download and use it.

Assuming I have access to "Check Me In", I intend to use it.

I intend to increase the use of "Check Me In" in the future.

I would appreciate using "Check Me In".

Willingness to disclose data (WILLINGNESS) was assessed by a single question adapted from Culnan and Armstrong (1999):

How likely would you provide your personal information (including your location) used in "Check Me In"? (From 0 to 100, where 0 = not at all; 100 = extremely likely)